PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-225143

(43)Date of publication of application : 17.08.1999

(51)Int.Cl.

H04L 9/32
G06F 17/60
G06K 17/00
G07B 1/00
G07B 5/00
G07F 7/12
G09C 1/00

(21)Application number : 10-027074

(22)Date of filing : 09.02.1998

(71)Applicant : FUJI XEROX CO LTD

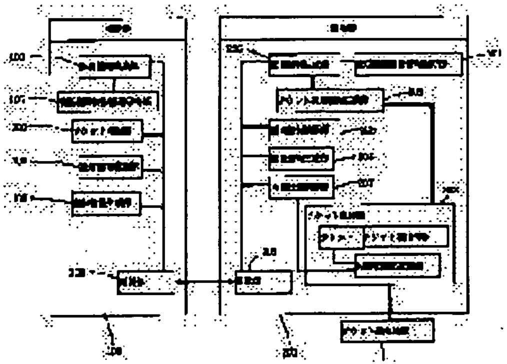
(72)Inventor : KIKO KENICHIROU
NAKAGAKI JUHEI
KIYOUJIMA HITOKI
TANIGUCHI SHINICHIRO

(54) ELECTRONIC TICKET SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an internal state of a certificate device from being revised due to a ticket exhibited by mistake or illegally.

SOLUTION: An authentication information generating section 102 of an authentication device 100 generates authentication information and sends it to a certificate device 200. A ticket discrimination information generating section 203 of the certificate device 200 generates ticket discrimination information to indicate storage of a correct ticket from ticket utilization information and information in an internal state storage area. A certificate information generating section 206 connects ticket discrimination information to low-order bits of a bit stream of the authentication information to generate ticket certificate information. The ticket certificate information is sent to the authentication device 100 by a communication section 208. The authentication device 100 receiving the ticket certificate information conducts ticket discrimination processing and terminates the protocol when the ticket certificate information is incorrect or the ticket is not to be authenticated.



LEGAL STATUS

[Date of request for examination]	20.09.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] It is the electronic ticket system which has certification equipment and verification equipment and verifies owning the ticket with the above-mentioned just certification equipment. The above-mentioned certificat equipment A certification equipment proper information maintenance means to hold the proper information on th above-mentioned certification equipment, and a ticket maintenance means to hold the above-mentioned ticket, T ticket judging information generation section which generates the ticket judging information that the content of access of the above-mentioned ticket or the busy condition of the above-mentioned ticket is expressed, Ticket confidential information is generated from the above-mentioned certification equipment proper information and t above-mentioned ticket at least. It has a certification information generation means to generate certification information using the above-mentioned ticket confidential information. The above-mentioned verification equipment A ticket judging means to judge whether I may perform verification processing based on the above-mentioned ticket judging information which the above-mentioned certification equipment presents, The electroni ticket system characterized by having a certification information verification means to verify whether the above-mentioned certification equipment has generated ticket confidential information based on the above-mentioned certification information.

[Claim 2] It is the electronic ticket system are an electronic ticket system according to claim 1, the above-mentioned verification equipment has an authentication information generation means generate the authenticatio information used by dialogue certification, and the certification information generation means of the above-mentioned certification equipment generates the above-mentioned certification information using the authenticat information which the above-mentioned verification equipment generated.

[Claim 3] It is the electronic ticket system which transmits the ticket judging information on a ticket that it is an electronic ticket system according to claim 2, and the above-mentioned certification equipment and the above-mentioned verification equipment have means of communications, and it is going to prove the above-mentioned certification equipment to the above-mentioned verification equipment.

[Claim 4] They are claim 2 thru/or an electronic ticket system given in 3. The above-mentioned electronic ticket system The above-mentioned verification equipment and the above-mentioned certification equipment are resembled, in addition it has ticket issuance equipment. The above-mentioned ticket issuance equipment A ticket description information maintenance means to hold the above-mentioned ticket confidential information which is the description information on the secrecy of the ticket to publish, and corresponding ticket public information, A certification equipment proper information maintenance means for ticket issuance to hold the proper information the above-mentioned certification equipment which a user holds, The electronic ticket system which has ticket issuance ****** which creates the ticket which is digital information using the above-mentioned ticket confiden information currently held for the above-mentioned ticket description information maintenance means, and the above-mentioned certification equipment proper information currently held for the above-mentioned certification equipment proper information maintenance means for ticket issuance.

[Claim 5] It is the electronic ticket system are claim 2 thru/or the electronic ticket system of 4, and the certificatio information generation means of the above-mentioned certification equipment is a predetermined approach, and calculates the ticket certification information use to the judgment of the above-mentioned ticket judging means a one of the above-mentioned certification information, from the authentication information sent from the above-mentioned verification equipment at least, the above-mentioned ticket, the above-mentioned ticket judging information, and the above-mentioned certification equipment proper information.

[Claim 6] It is the electronic ticket system which are an electronic ticket system according to claim 5, and the above-mentioned certification equipment makes the ticket utilization information that the utilization conditions o ticket were defined correspond with a ticket, and holds to the above-mentioned ticket attaching part.
[Claim 7] It is the electronic ticket system which uses the above-mentioned ticket utilization information at least case it is an electronic ticket system according to claim 5 and the above-mentioned certification equipment create the above-mentioned ticket judging information.
[Claim 8] It is the electronic ticket system which is an electronic ticket system according to claim 6, and is equipped with the internal-state storage region holding a strange internal state with the above-mentioned good certification equipment, and the internal-state control means which controls the value of the above-mentioned internal state.
[Claim 9] It is the electronic ticket system which uses the information on the internal-state storage region of the above-mentioned certification equipment at least in case it is an electronic ticket system according to claim 8 and the ticket judging information generation means of the above-mentioned certification equipment creates the abov mentioned ticket judging information.
[Claim 10] It rewrites from the outside and at least the part of the strange good internal states which are claim 8 thru/or the electronic ticket system of 9, and the internal-state storage region of the above-mentioned certification equipment holds is a impossible electronic ticket system.
[Claim 11] It is the electronic ticket system by which it is claim 8 thru/or the electronic ticket system of 10, and t certification information generation means of the above-mentioned certification equipment calculates the above-mentioned certification information at least using the above-mentioned ticket, the above-mentioned ticket utilization information, and the above-mentioned certification equipment proper information.
[Claim 12] It is the electronic ticket system are claim 8 thru/or the electronic ticket system of 11, and above-mentioned certification equipment has the authentication information maintenance means hold the above-mentioned authentication information sent from the above-mentioned verification means, and the above-mention certification information generation means changes the authentication information currently held at the above-mentioned authentication information maintenance means using the ticket judging information generated by the above-mentioned ticket judging information generation means, and use to generation of the above-mentioned certification information.
[Claim 13] When ticket judging information which is the electronic ticket system of claim 12 and the above-mentioned ticket judging information generation means generated is set to M and the above-mentioned authentication information sets to C, the certification information generation means of the above-mentioned certification equipment is the electronic ticket system which updates to what joined M to C in the authentication information C currently held at the above-mentioned authentication information maintenance means.
[Claim 14] They are claim 12 thru/or the electronic ticket system of 13. The certification information generation means of the above-mentioned certification equipment It is possible to generate ticket certification information a one of the above-mentioned certification information. The above-mentioned ticket certification information The electronic ticket system generated by calculating ticket confidential information by the predetermined approach from the above-mentioned ticket, the above-mentioned ticket utilization information, and the above-mentioned certification equipment proper information, and performing count using ticket confidential information to the above-mentioned authentication information.
[Claim 15] It is the electronic ticket system of claim 14, p and q are the prime factors, and it is n=p-q, and is DE**1. mod (p-1) (q-1) When relation is filled, The above-mentioned ticket confidential information is D, ticket public information is (n, E), the above-mentioned ticket utilization information is L, the above-mentioned certification equipment proper information is the value du of secrecy, and, on the other hand, f (du, L, n) is made into a tropism function. When the ticket is given by t=D-f (du, L, n), the certification information generation mea of the above-mentioned certification equipment As opposed to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed) the law of C -- the power by t in n, and the law of C -- law with the power in n according to the tropism function valu (du, L, n) on the other hand -- product CtCf in n (du, L, n) mod Electronic ticket system which calculates ticket certification information as n.
[Claim 16] It is the electronic ticket system of claim 14, p and q are the prime factors, and it is n=p-q, and is DE**1. mod (p-1) (q-1) When relation is filled, The above-mentioned ticket confidential information is D, ticket public information is (n, E), the above-mentioned ticket utilization information is L, the above-mentioned

certification equipment proper information is the value du of secrecy, and, on the other hand, f (du, L, n) is made into a tropism function. When the above-mentioned ticket is given by t=D-f (du, L, n), the above-mentioned certification equipment t+f(du, L, n) =D is calculated beforehand, the value is used, and it is T=CD to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed). mod Electronic ticket system which calculates the ticket certification information T as n.

[Claim 17] the electronic ticket system of claim 14 -- it is -- g -- dispersion -- a logarithm -- the primitive root of group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer x -- receiving -- y=gxmod When is realized The above-mentioned ticket confidential information is x, ticket public information is (y, p, g), the above-mentioned ticket utilization information is L, the above-mentioned certification equipment proper information is the value du of secrecy, and, on the other hand, f (du, L, y) is made into a tropism function. When above-mentioned ticket is given by t=x-f (du, L, y), the above-mentioned certification equipment As opposed to above-mentioned authentication information C (authentication information which the above-mentioned certificat information generation means changed) the above-mentioned ticket judging information T -- the law of C -- the power by t in p, and the law of C -- law with the power in p which, on the other hand, makes a characteristic the tropism function value f (du, L, y) -- product CtCf in p (du, L, y) Electronic ticket system which calculates the above-mentioned certification information as modn.

[Claim 18] the electronic ticket system of claim 14 -- it is -- g -- dispersion -- a logarithm -- the primitive root of group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer x -- receiving -- y=gxmod When is realized The above-mentioned ticket confidential information is x, ticket public information is (y, p, g), the above-mentioned ticket utilization information is L, the above-mentioned certification equipment proper information is the value du of secrecy, and, on the other hand, f (du, L, y) is made into a tropism function. When above-mentioned ticket is given by t=x-f (du, L, y), the above-mentioned certification equipment It is Cx, in case t+f(du, L, y) =x are calculated beforehand and the ticket (authentication information which above-mentioned certification information generation means changed) judging information T is calculated to the above-mentioned authentication information C. mod Electronic ticket system using the value of p.

[Claim 19] It is the electronic ticket system are claim 14 thru/or the electronic ticket system of 18, and the certification information verification means of the above-mentioned verification equipment verifies the justificat of the above-mentioned ticket certification information from the authentication information which the above-mentioned authentication information generation means created, the ticket certification information which were sent from the above-mentioned certification equipment, and the above-mentioned ticket public information, and right case derives the ticket judging information were embedded to the above-mentioned ticket certification information, in the above-mentioned ticket certification information.

[Claim 20] It is the electronic ticket system of claim 19, and the above-mentioned authentication information is C When the above-mentioned ticket certification information is T, it is the above-mentioned ticket public informati (n, E) and there is certain bit string M, the certification information verification means of the above-mentioned verification equipment the above-mentioned ticket certification information T -- law -- the bit string which joined and M for what carried out the exponentiation by E by n -- comparing -- TE mod If it is n=C||M (notation || is junction of a bit string) It is the electronic ticket system by which the above-mentioned ticket certification information is judged to be the right, and the above-mentioned ticket certification information derives M as the above-mentioned ticket judging information in a right case.

[Claim 21] It is the electronic ticket system of claim 19, and the above-mentioned authentication information is C When the above-mentioned ticket certification information is T and the above-mentioned ticket public informatio is (p, g, y), the certification information verification means of the above-mentioned verification equipment

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the technique of creating a ticket and a card electronically and using them.
[0002]
[Background of the Invention] The attempt which publishes common tickets, such as a ticket, an admission ticke reserved seat ticket, a reservation ticket, a coupon ticket, a commuter pass, a prepaid card, and a point card, as an electronic ticket is performed in recent years [[conventional technical]].
[0003] A publisher can specify the access granted to the user and such an electronic ticket has the function in wh it is verifiable that it is a right ticket. Electronic intelligence is easy to create, and although it has the features that can transmit through a communication line, since it can make a perfect copy easily, the cure to the unjust utilizat by forgery and the duplicate is indispensable [electronic intelligence] to implementation of an electronic ticket. Although prevention of forgery by electronic signature is possible, prevention of a duplicate is difficult, and preventing the unjust utilization by the duplicate had become the biggest technical problem were in charge of implementation of an electronic ticket.
[0004] The three approaches of of the user just to the utilization time of the former and a ticket as a solution, the conventional technique to check, the 2nd conventional technique which does not give an opportunity to copy a ticket at persons other than a publisher, and the 3rd conventional technique which corrected the 2nd conventiona technique so that the communication link at the time of verification could be exhibited over this problem have be proposed.
[0005] The 1st conventional technique is the approach a user checks whether you are a just user to the utilization time of a ticket, and a user shows with a ticket that he is the just user to whom he suits user specific information, when using a ticket. If it conforms to user specific information, use of corresponding access will be accepted. Information which matches information (user specific information) required for a check and the granted access is published as a ticket, and a user keeps records. In order for persons other than a publisher to prevent from forging ticket freely, a publisher performs electronic signature to a ticket. The ticket without electronic signature is judge to be what was forged. Possession of the information of the bodily features of an identity, a photograph of his fac etc., a password, etc. can be used for user specific information.
[0006] However, by this approach, some troubles arise according to the user specific information to be used.
[0007] For example, by the approach of using a user's identity for user specific information, a user will be identif at the time of issuance and verification, and anonymity will be lost. Moreover, since the method of proving a stat safely in the remote environment using a communication line is not realized, in such an environment, a thing without just access cannot prevent using a ticket unfairly.
[0008] Although the problem of anonymity will be mitigated if a password is used for user specific information, load which memorizes a password is given to a user. Moreover, since it cannot prevent that a user makes a password reveal intentionally, there is also a trouble that the risk of unjust utilization will increase.
[0009] The 2nd conventional technique is the approach of not giving an opportunity copying a ticket to persons other than a publisher as is shown in JP,8-147500,A. By this approach, both the device which prevents from copying the ticket in which the user is doing maintenance management, and the device which a ticket does not reveal from the communication link at the time of issuance and verification are needed.
[0010] However, by this approach, since persons other than (1) publisher also carry out the content of the

communication link at the time of issuance of (2) tickets with which it becomes difficult to prove the justification a ticket for a third party since a ticket cannot be copied, and verification to secrecy, the trouble that it cannot prov not infringing on the access of users, such as privacy, at the time of issuance of a ticket and verification arises.

[0011] The 3rd conventional technique is the approach which corrected the 2nd conventional technique so that th communication link at the time of verification can be exhibited, as shown in JP,6-52518,B. Although it records th it cannot copy to the equipment (certification equipment) which a user possesses by making a ticket into confidential information like the 2nd conventional technique by this approach, the approaches of verification diff First, the verification equipment which verifies sends values (challenge) by which repeat utilization is not carried out, such as a random number, to certification equipment. Certification equipment performs the operation using t confidential information which is a ticket to a challenge, and returns the acquired value (response) to verification equipment. Verification equipment is checking what the response's calculated using confidential information and challenge, and attests a user's justification. It becomes unnecessary to let a challenge and a response be secret communication from a response by making it difficult in computational complexity to ask reverse for confidentia information.

[0012] This approach is used for authentication and information is not transmitted [whether the just ticket is held and] to except. For this reason, an expiration date etc. cannot be shown but only a simple ticket can be expressed Moreover, there was a problem that it could not prove that the method of transmitting a ticket to certification equipment needs to carry out by secret communication link like the 2nd conventional technique, discloses a user' information unfairly, and is not infringing on a user's access.

[0013] Thus, each Prior art had a problem in the point at the sacrifice of the function of a ticket of content certification and a user's anonymity to a third party, in order to realize the function to prevent unjust utilization required for a ticket.

[0014] [Related technique] The approach shown in Japanese Patent Application No. No. (un-opening [July 14, Heisei 9,] to the public) 188064 [nine to] is proposed as a related technique which solves these problems.

[0015] The general Challenge Handshake Authentication Protocol of this related technique is shown in drawing 1 This protocol is a protocol which performs bidirectional authentication, and when both sides check the signature authentication information (generated random number), it attests each other justification. Informational safe trans is enabled by including a message (m, mu) in a part of mutual authentication information (random number).

[0016] The protocol of a related technique is explained with reference to drawing 1 . In drawing 1 , first, verification equipment generates the authentication information C based on a random number (S11), and this authentication information C is sent to certification equipment (S12). On the other hand, certification equipment generates another authentication information chi based on a random number, and sends the authentication information chi to verification equipment (S13, S14). Corresponding to a ticket, there is an internal state which cannot be operated in certification equipment from the exterior, and it can rewrite only by the response indication from verification equipment. The response indication in which the information (mu) to which modification of an internal state is permitted was included is created to a part of chi, verification equipment signs it, and verification equipment is sent to it at certification equipment (S15, S16). By checking the signature of a response indication r a transmitting person checks that it is just verification equipment, and, as for certification equipment, checks the rightness of the information mu on internal-state modification with it (S17). The internal state of certification equipment is changed only into a right case for rho according to the content of mu (S18). The service set to verification equipment by performing a signature it being possible to restore D (S19) and according to D to the certification information R at the last when delivery (S20, S21) and verification equipment checked the signature offered from Ticket t and the certification equipment proper information du that certification equipment was crea justly (S22, S23).

[0017] According to this approach, since the verification information on a ticket is disclosure, verification of a ticket is possible for it also to the 3rd person, and since a user does not have the need of showing the information which specifies a user at the time of verification of a ticket, anonymity is also kept.

[0018] Moreover, when verification equipment and certification equipment share each of each other's confidentia information and public information and carry out mutual authentication, the problem of forgery of certification equipment and verification equipment is solved. Furthermore, by embedding information transmitting to a part o authentication information used for this certification, signal transduction verification equipment and between certification equipment is also made possible, and the content of the ticket can be proved.

[0019] Thus, if the approach of this related technique is used, the safe electronic ticket which filled all the fundamental functions of an electronic ticket can be realized, and it is possible to solve all the above-mentioned problems.
[0020] By the way, with the previous related technique, it is premised on the ticket which verification equipment tends to verify becoming settled uniquely in certification equipment by sending the information as which verification equipment specifies a ticket to certification equipment. However, it is also considered actually that tw or more tickets verifiable [with the verification equipment] exist in certification equipment. For example, when thing like the ticket of a railroad is considered, two or more tickets, such as a valid coupon ticket, a valid commu pass, etc., may exist in certification equipment from the station. In such a case, with certification equipment, it cannot judge which ticket the user is going to use. Then, the need of choosing the ticket which a user uses beforehand in such cases arises.
[0021] And in such a scene, if a previous related technique is applied, the problem that it will be created and the response indication to which modification of the internal state corresponding to a ticket is permitted will be sent, without checking the content of the ticket chosen and shown will arise.
[0022] This means that the internal state of the ticket which is not meant will be changed, when the ticket which user mistook has been chosen.
[0023] Moreover, considering the case where it applies to the ticket of a railroad, it is possible by leaving record entrance and checking record of entrance as an internal state, at the time of participation to prevent a malfeasance like cheating on the fare.
[0024] Here, a case so that it may leave only the data of having only come in to the internal state corresponding t ticket, as information on entrance is considered. In such a case, if it sends to certification equipment, without checking the modification authorization information on an internal state, and the content of the ticket specifically shown entrance information, originally it will become possible to leave the data of having come in at the station also to the ticket which cannot come in. If the entrance record over the ticket from the station near [station / whi came in actually] the object station will forge supposing it can get the certification equipment holding the ticket with which it is the phase where of entrance was refused and the internal state was rewritten, although entrance w the ticket which is not just cannot be performed actually, it is showing a ticket with the entrance record forged at time of participation, and a cheating-on-the-fare act will become possible.
[0025] Thus, when a user chooses himself the ticket which it is going to prove, verification equipment needs to check that the shown ticket can verify justly with the verification equipment, before creating the authorization information which changes an internal state.
[0026] However, in a previous related technique, in order that such a check might not accomplish, there was a trouble that rewrote the internal state corresponding to the ticket which a user does not mean accidentally, or the injustice by rewriting an internal state was possible.
[0027]
[Problem(s) to be Solved by the Invention] It aims at realizing an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right in this invention in order to solve the above-mentioned problem.
[0028]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the electronic ticket system concerning this invention It consists of ticket verification equipment and certification equipment. Ticket verification equipment A ticket judging means to judge whether the ticket to verify can verify with verification equipment based on the ticket judging information which certification equipment presents, It has a dialogue verification means to verify whether certification equipment has computed ticket confidential information. Certification equipment It has at least the certification equipment proper information maintenance means, the tick maintenance means, and a dialogue certification means by which information about ticket confidential informatio can be proved, from certification equipment proper information and a ticket.
[0029] In this configuration, verification equipment can check the compatibility of the ticket in certification equipment based on ticket judging information, and only when a right ticket is shown, the internal state of certification equipment can be changed.
[0030]

[The mode of implementation of invention] Hereafter, this invention is explained to a detail.
[0031] Electronic ticket structure-of-a-system drawing of the example 1 of this invention is shown in [example 1 drawing 2 . In drawing 2 , the electronic ticket system shown in this example consists of verification equipment (is also called a verification machine) 100, certification equipment (it is also called a certification machine) 200, a ticket assignment equipment 300.
[0032] Verification equipment 100 is constituted including the ticket judging section 101 which judges the justification of the ticket to verify, the authentication information generation section 102, the certification information generation section 103, the certification information verification section 104, the verification equipment privilege information attaching part 105, and the communications department 106.
[0033] On the other hand, certification equipment 200 is constituted including the certification equipment proper information attaching part 201, the ticket attaching part 202, the ticket judging information generation section 20 the authentication information generation section 204, the certification information verification section 205, the certification information generation section 206, the internal-state control section 207, and the communications department 208. In addition, the certification information generation section 103 of verification equipment 100 a the certification information generation section 206 of authentication equipment 200 possess the storage section holding the authentication information sent from authentication equipment 200 and verification equipment 100, respectively.
[0034] Moreover, a ticket and the ticket utilization information corresponding to each ticket are saved at the ticke attaching part 202. Moreover, the internal-state storage region corresponding to each ticket is secured to the ticke attaching part 202.
[0035] Here, certification equipment 200 is constituted by medium like an IC card with it difficult [to observe internal data and processing procedure from the outside].
[0036] Moreover, in this example, Ticket t is published as follows.
[0037]
[A table 1]
Ticket: $t=D-F(n, L, du)$
D: the confidential information n:ticket method of a ticket private key du:certification equipment proper -- severa F:un-colliding nature one-way function L:ticket utilization information, however ED**1mod n -- it is E:ticket public key here. Ticket confidential information is D and ticket public information is E, n, and L. F is realizable with a general Hash Function. Moreover, the information on the conditions using the ticket, for example, an expiration date, the location which can receive service goes into the ticket utilization information L.
[0038] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 3 First, after a user specifies the ticket to be used from now on as certification equipment 200 with ticket assignme equipment 300, Challenge Handshake Authentication Protocol is started between verification equipment 100 and certification equipment 200.
[0039] In drawing 3 , by Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number C as authentication information and sends to certification equipment 200 (S31, S32).
[0040] The certification equipment 200 which received authentication information performs ticket certification information generation processing (S33).
[0041] The flow chart of ticket certification information generation processing (S33) is shown in drawing 4 . In drawing 4 , the certification information generation section 206 of certification equipment 200 computes first the private key D used for a signature by the following count from the certification equipment proper information du saved at Ticket t, the ticket utilization information L, and the certification equipment proper information attachin part 201 (S41).
[0042]
[Equation 7]
$t+F(n,L,du)$
$=D-F(n,L,du)+F(n,L,du)$
= Generate the ticket judging information M to show that D, next the ticket judging information generation sectio 203 hold the right ticket from the ticket utilization information on the ticket attaching part 202, and the informati on an internal-state storage region (S42). The certification information generation section 206 connects the ticket

judging information M with the low order of the bit string of the authentication information C (S43), and is the ticket certification information T [0043]
[Equation 8] T=(C||M) D mod Count of n generates (in addition, S44 and connecting notation || with a bit string a shown). In addition, besides the above-mentioned count, it is [0044].
[Equation 9]
T=(C||M) t(C||M) F (n, L, du) mod The certification information T may be calculated by n.
[0045] Moreover, the authentication information generation section 204 generates a random number chi, and is taken as the 2nd authentication information (S44).
[0046] The ticket certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208 (S34). Ticket certification information is a right thing and signs for guaranteeing that certification equipment and ticket judging information are not forged.
[0047] The verification equipment 100 which received T and chi performs ticket judging processing (S35 of drawing 3).
[0048] The flow chart of ticket judging processing (S35 of drawing 3) is shown in drawing 5 . It is [0049] from t ticket certification information T that the certification information verification section 104 of verification equipment 100 was sent in drawing 5 , and the ticket public information E which the certification information verification section holds.
[Equation 10] TE mod The value of n is calculated and it checks whether the part of the high order bit connected among the bit string is in agreement with the authentication information C (S51). When in agreement, the ticket judging information M is extracted further (S52). Next, the ticket judging section 101 judges whether it is what th internal state related with the ticket and the ticket based on the content of M may verify with this verification equipment (S53). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with the low order of chi (S54, S55). Furthermore, the value rho which signed us the confidential information delta showing the privilege of verification equipment is created to this value (S56). Created rho is sent to certification equipment 200 by the communications department 106 (S36).
[0050] On the other hand, when ticket certification information is not a right thing, or in being what a ticket shou not verify, it ends a protocol (S57).
[0051] Next, the certification equipment which received rho performs internal-state modification processing (S37 drawing 3).
[0052] The flow chart of internal-state modification processing (S37 of drawing 3) is shown in drawing 6 . To th 2nd certification information rho that the certification information verification section 205 of certification equipment 200 was sent in drawing 6 , the public information epsilon which checks the privilege of the verificati equipment 100 which self holds is used, and it is [0053].
[Equation 11]
$\rho^{\varepsilon} \bmod \nu$

It calculates and checks whether the part of a high order is in agreement with the 2nd authentication information among the bit string (S61). As a result of a check, when it becomes clear that it is not right, a protocol is ended to case (S62). Connected mu is extracted when it is able to be checked that it is a right thing (S63). The internal-sta control section 207 changes the internal state of certification equipment 200 according to the content of mu, and makes the result M' (S64, S65). The certification information generation section 206 is [0054] after connecting th value of M' with the bit string of the authentication information C.
[Equation 12] R=(C||M') D mod Count of n generates the certification information R (S66, S67). R is sent to verification equipment 100 by the communications department 208 (S38).
[0055] The verification equipment 100 which received R performs certification information verification processi (S39 of drawing 3).
[0056] The flow chart of certification information verification processing (S39 of drawing 3) is shown in drawin 7 . The ticket public information E which the certification information verification section 104 of verification equipment 100 holds in drawing 7 is used, and it is [0057].
[Equation 13] RE mod The value of n is calculated and the bit string of the high order except M' connected as a result checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S71). The defined service is offered, when it checks whether the content of information M' which

expresses the modification result of an internal state further is in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S72, S7 S74) and a check is completed (S75). When one of checks goes wrong, a protocol is completed and offer of servi is not performed (S71, S74, S76).

[0058] The example 2 of [example 2] this invention is the case where an example 1 is realized as a ticket of the ticket of a railroad. The protocol at the time of entrance of a ticket is explained especially here.

[0059] Although the configuration of the example of this invention and the generation method of a ticket are the same as that of an example 1, verification equipment 100 is specifically an automatic ticket gate, and certification equipment 200 is a token like an IC card which can hold a ticket. And verification according to an automatic wic in entrance and participation shall be performed, and the storage region corresponding to entrance or participatio shall be secured to an internal state.

[0060] Below, the example of the ticket on Yokohama - Narita Airport July 18, 1997 explains. In addition, the st to which drawing 3 corresponds is pointed out suitably.

[0061] The ticket utilization information L on a ticket becomes like drawing 9 . The ticket is registered into certification equipment 200 and the corresponding internal-state storage region is secured. The internal state befo entrance is shown in drawing 8 . Here, Ticket ID shows the ticket to be used from now on to 00005.

[0062] First, the authentication at the time of entrance is explained. Verification equipment 100 sends the information showing being entrance to certification equipment 200 with the authentication information C first (S32).

[0063] Certification equipment 200 generates the ticket judging information M. The content of M is shown in drawing 10 . As shown in drawing, the content included in ticket utilization information and the content of entrance / participation record of an internal state to show a busy condition are included in the ticket judging information M. The certification information generation section 206 connects M with C, performs the signature b the ticket private key D, and sends it to verification equipment 100 with the 2nd generated authentication information chi as ticket certification information T (S34).

[0064] Verification equipment 100 verifies ticket certification information, and checks the content of the ticket judging information M further. Here, since an entrance station is within an expiration date and is an intact ticket the Yokohama station, it is judged with it being the ticket which may carry out authentication here (S35).

[0065] Then, the information mu for changing the internal state of certification equipment 200 is created. The content of mu is shown in drawing 11 . An entrance name of the station and time amount are recorded on mu. Th certification information generation section 103 connects with the 2nd authentication information chi mu generat in this way, generates the value rho which performed the signature using the privilege information delta on verification equipment 100, and sends it to certification equipment 200 (S36).

[0066] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When it is able to be checked that it is a right thing, the internal-state control section 207 changes the internal state of certification equipment 200 according to the content of mu (S37). The situation of the internal state after modification is show in drawing 12 . It turns out that the station and time amount of entrance were recorded. Next, the internal-state control section 207 makes M' the content of modification of this internal state, i.e., entrance record. Like an example 1, the certification information generation section 206 connects the value of M' with the bit string of authentication information, generates the value R which performed the signature by ticket confidential informatio and sends it to verification equipment 100 as certification information R (S38).

[0067] When the value of the certification information R is verified and the value is in agreement with the authentication information C, verification equipment 100 checks M', as a result of changing an internal state furth If M' corresponds with what was specified by mu, it will be judged as that by which the internal state was change correctly, and the gate of a ticket gate machine will be opened.

[0068] Next, the authentication at the time of participation is explained. Although the authentication at the time o participation is the same as that of the time of entrance almost, the contents of the message told mutually differ.

[0069] Verification equipment 100 sends the information showing being participation to certification equipment with the authentication information C first (S32).

[0070] The ticket judging information generation section 203 of certification equipment 200 generates the ticket judging information M. The content of M at the time of participation is shown in drawing 13 . The certification

information generation section 206 connects M with C, performs the signature by the ticket private key D, and is taken as the ticket certification information T. And the 2nd authentication information chi which carried out authentication information generation section generation with the certification information T is sent to verificatio equipment (S34).
[0071] The certification information verification section 104 of verification equipment 100 verifies ticket certification information. In a verification result [of a ticket], or right case, the ticket judging section 101 checks the content of the ticket judging information M. Here, since an entrance station is effective entrance record and is within the shelf-life of participation at the Yokohama station, it is judged with it being the ticket which can attest participation here (S35).
[0072] Next, the certification information generation section 103 creates the information mu for changing the internal state of certification equipment 200. The content of mu is shown in drawing 14 . A participation name of the station and participation time amount are recorded on mu. The certification information generation section 10 connects generated mu with chi further, and generates the value rho which performed the signature using the privilege information delta on verification equipment. rho is sent to certification equipment 200 (S36).
[0073] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When the right thing is a to be checked, according to the content of mu, the internal-state control section 207 changes the internal state of certification equipment 200, and makes it M' as a result of [this] modification (i.e., participation record). The situation of the internal state after modification is shown in drawing 15 . A participation station and time amount are recorded. The certification information generation section 206 connects participation record M' with the bit string of the authentication information C, generates the certification information R which performed the signatu by ticket confidential information, and sends it to verification equipment 100 (S38).
[0074] When the value of R is verified and the value is in agreement with the authentication information C, the certification information verification section 104 of verification equipment 200 checks M', as a result of changing an internal state further. If M' corresponds with what was specified with the value of mu, it will be judged as that which the internal state was changed correctly, participation will be permitted, and the gate of a ticket gate mach will be opened (S39).
[0075] The [example 3] example 3 shows how to realize a gestalt like a coupon ticket.
[0076] Fundamentally, the configuration of this example, the generation method of a ticket, and the flow of the whole processing are the same as that of an example 1. The configuration of whole this example is shown in drawing 16 . It differs in that counter 202a which shows the remaining frequency of a coupon ticket is installed in the internal state as a description of this example. In drawing 16 , the sign corresponding to drawing 2 and a corresponding part was attached.
[0077] A user will register with certification equipment 200 first, if a coupon ticket is purchased. The internal-sta storage region corresponding to a coupon ticket is secured at the time of registration, and the remaining use coun are written in counter 202a in it.
[0078] After a user specifies a coupon ticket with ticket assignment equipment 300 as a ticket used to certificatio equipment 200 after this, Challenge Handshake Authentication Protocol is started by the utilization time of a coupon ticket between verification equipment 100 and certification equipment 200.
[0079] At Challenge Handshake Authentication Protocol, it is the same as that of an example 1 till the place whe verification equipment 100 generates a random number C as authentication information at, and delivery and certification equipment 200 calculate a ticket private key to certification equipment 200.
[0080] The flow chart of ticket certification information generation processing (it corresponds to R> 3 drawing 3 S33) of this example is shown in drawing 17 . In drawing 17 , the ticket judging information generation section 2 of certification equipment 200 extracts the count of the remainder of the internal state corresponding to the ticket this coupon ticket, and records it on the ticket judging information M with ticket utilization information (S81-S84 And like an example 1, the certification information generation section 206 generates the ticket certification information T (S85), and the authentication information generation section 204 generates the 2nd authentication information chi (S86). T and chi are sent to verification equipment 100 by the communications department 208 (S34).
[0081] The verification equipment 100 which received T and chi performs ticket judging processing (it is ****** S35 of drawing 3).

[0082] The flow chart of ticket judging processing is shown in drawing 18 R> 8. In drawing 18 , the certification information verification section 104 of verification equipment 100 verifies the received ticket certification information (S91). Ticket certification information extracts the ticket judging information M from ticket certification information to a right case (S92). The count of the remainder of a coupon ticket is recorded on the ticket judging information M. With [that value] one [or more], the ticket judging section 101 judges that this coupon ticket is still usable (S93). Furthermore, when the ticket judging section 101 also judges [that it is verifia with this verification equipment 100 and] the content of the ticket utilization information L, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200 (S94, S95). The content which directs to reduce the use count of a coupon ticket by o as a content of mu is included. And by the same approach as an example 1, the 2nd certification information rho created using mu (S96, S97), and it sends to certification equipment 200 (S36).

[0083] Error processing is performed when verification and a ticket judging go wrong (S98).

[0084] The certification equipment 200 which received rho performs internal-state modification processing (it corresponds to S37 of drawing 3).

[0085] The flow chart of internal-state modification processing is shown in drawing 19 R> 9. In drawing 19 , the certification information verification section 205 of certification equipment 200 verifies the 2nd sent certification information rho (S101). When it is able to be checked that it is a right thing, according to the content of mu, an internal-state control section reduces the remaining use count of a coupon ticket by one, and makes the result M' (S102-S104). The rest is the same approach as an example 1, and certification equipment 200 generates the certification information R, and sends it to verification equipment 100 (S105, S106). Error processing is perform when verification goes wrong at step S101 (S107).

[0086] Actuation of the subsequent verification equipments 100 is the same as that of an example 1, verifies the value of R and offers service.

[0087] In the example 4 of [example 4] this invention, although the whole configuration is the same as that of an example 1, the authentication approaches of ticket public information and ticket confidential information, or a tic differ.

[0088] this example -- p -- the prime factor -- it is -- G -- dispersion -- a logarithm -- a finite group with a difficul problem -- it is -- g -- the origin of the order p of a finite group G -- it is -- [0089]

[Equation 14] y=gx mod When p is filled, (p, G, g, y) are ticket public information, and make x ticket confidentia information. (p, G, g) can also be made common by the whole system.

[0090] At this time, a ticket is [0091] from the ticket description information x, the certification equipment prope information du, the ticket utilization information L, and the information p that specifies a group.

[Equation 15] t=x-F(du,L,y,p)

It is calculated by carrying out. Here, F is the one-way function of un-colliding nature, and a general Hash Functi can realize it. L is the same ticket utilization information as an example 1.

[0092] Moreover, the above (p, G, g) is [0093] as common as a thing showing the privilege of verification equipment.

[Equation 16]

$$\eta = g^{\xi} \bmod p$$

******** -- let eta [like] into public information and let xi be confidential information.

[0094] G can be actually constituted as a multiplicative group, or it can constitute as an elliptic curve on finite fie

[0095] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 20

[0096] First, after a user specifies the ticket to be used from now on to certification equipment, Challenge Handshake Authentication Protocol is started between verification equipment and certification equipment.

[0097] In drawing 20 , by this Challenge Handshake Authentication Protocol, first, the authentication informatio generation section 102 of verification equipment 100 generates a random number r, calculates C=gr, and sends to certification equipment by making this into authentication information (S201, S202, S203).

[0098] The certification equipment 200 which received the authentication information C performs ticket certification information generation processing (S204).

[0099] The flow chart of ticket certification information generation processing is shown in drawing 21 . In drawi 21 , the certification information generation section 206 of certification equipment 200 computes first the private

h c g cg b eb cg e e

key x used for a signature by the following count from p of Ticket t, the ticket utilization information L, and tick public information, and the certification equipment proper information du (S211).
[0100]
[Equation 17]
t+F(y,L,du,p)
=x-F(y,L,du,p)+F(y,L,du,p)
= Generate the ticket judging information M to show that x, next the ticket judging information generation sectio 203 hold the right ticket from the additional information L of a ticket, and the information on an internal state (S212). The certification information generation section 206 generates the following values as certification information (S213, S214).
[0101]
[Equation 18] T= (C||M) and Cx mod p -- in addition, the certification information T is calculable with the following formulas besides the above.
[0102]
[Equation 19]
T= (C||M) and CtCF (y, L, du, p) mod p and the authentication information generation section 204 generate random-number r' simultaneously, and are [0103].
[Equation 20] Chi=gr' mod p is sent to verification equipment as 2nd authentication information (S215, S216, S205). The information included in the ticket judging information M is the same as that of examples 1-3.
[0104] The certification information T and the 2nd authentication information chi are sent to verification equipm 100 by the communications department 208.
[0105] The verification equipment 100 which received T and chi performs ticket judging processing (S206 of drawing 20).
[0106] The flow chart of ticket judging processing is shown in drawing 22 R> 2. It is [0107] from the ticket certification information that the certification information verification section 103 of verification equipment 100 was sent in drawing 22 .
[Equation 21] T/yr mod p= (C||M) and Cx/yr mod The value of p is calculated and it checks whether parts other than M connected among the bit string are in agreement with the authentication information C (S221). When in agreement, the ticket judging section 101 judges further whether it is what the internal state related with the ticke and the ticket may verify with this verification equipment 100 from the content of the ticket judging information (S222, S223). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with chi (S224, S225). And the following values are generated as 2nd authentication information to this value using the confidential information xi showing the privilege of verification equipment (S226).
[0108]
[Equation 22]
$\rho = (\chi \mid \mid \mu) \cdot \chi^{\xi} \mod p$

rho is sent to certification equipment 200 by the communications department 106. On the other hand, when ticke certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S227)
[0109] Next, the certification equipment 200 which received rho performs internal-state modification processing (S208 of drawing 20).
[0110] The flow chart of internal-state modification processing is shown in drawing 23 R> 3. It is [0111] from a response indication to which the certification information verification section 205 of certification equipment 200 was sent in drawing 23 .
[Equation 23]
$\rho / \eta^{r'} \mod p = (\chi \mid \mid \mu) \cdot \chi^{\xi} / \eta^{r'} \mod p$

A ** value is calculated and it checks whether parts other than mu connected among the bit string are in agreeme with the 2nd authentication information chi (S231). When it is able to be checked that it is a right thing, accordin to the information the internal-state control section 207 instructs modification of the internal state of mu to be, th internal state of certification equipment 200 changes and the result is made into M' (S232-S234). On the other ha

as a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S137).
[0112] after the certification information generation section 206 connects the value of M' with the bit string of th authentication information C -- the following values -- certification information -- ** -- it generates by carrying o (S235, S236).
[0113]
[Equation 24] R= (C||M') and Cx mod p -- the certification information R generated in this way is sent to verification equipment 100 by the communications department 208 (S209).
[0114] The verification equipment 100 which received R performs certification information verification processi S210 (drawing 20).
[0115] The flow chart of certification information verification processing is shown in drawing 24 R> 4. It is [011 from the ticket certification information that the certification information verification section 104 was sent in drawing 24 .
[Equation 25] R/yr mod The value of p= (C||M') and Cx/yrr mod p is calculated and, as a result, the bit string of t high order except M' checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S241). The defined service is offered, when it checks whether the content of information M' which expresses the modification result of an internal state further is in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when i able to check (S242, S243, S244) and a check is completed (S245). When one of checks goes wrong, a protocol i completed and offer of service is not performed (S246).
[0117]
[Effect of the Invention] As explained above, according to this invention, an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information which modification of an internal state is permitted to the ticket which is not right can be realized, and the malfeasance by modification of the internal state which a user does not mean, and modification of an internal sta can be prevented.

[Translation done.]